



## 【特許請求の範囲】

【請求項 1】 IC 内部のデータ格納領域に格納されたデータの更新制御手段を有する IC カードと、この IC カードの格納データに対応する内部管理データの更新制御手段を有する第 1 装置と、前記 IC カード及び第 1 の装置の各更新制御手段に対してデータ更新要求を発行する第 2 装置とを含んで構成される IC カードシステムにおいて、前記第 2 装置に、前記 IC カードの更新制御手段へ前記格納データの仮更新を要求する仮更新要求発行手段と、該仮更新の正常終了を確認したときに前記第 1 装置の更新制御手段へ内部管理データの実更新を要求する実更新要求発行手段と、該内部管理データの実更新の正常終了を確認したときに前記 IC カードの更新制御手段へ本更新を要求する本更新発行手段とを設け、この本更新の実行によって前記 IC カード内の格納データの内容を確定させるようにしたことを特徴とする IC カードシステム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、カード発行主体であるセンタシステムで管理するデータとの更新状態の整合性が図れない場合に、格納データへのアクセスを制限する機能を有する IC カード、及びこの IC カードを使用した IC カードシステムに関する。

## 【0002】

【従来の技術】 IC カードの内部に、カード発行主体であるセンタシステム側で管理されている対象データ、例えば金額等に相当するデータ（以下、金額データ）を格納しておき、その金額データを用いてセンタシステム側の了解を得ずに商品購入等を行う取引形態がある。このような取引形態をオフライン取引という。例えば、センタシステムとオンライン接続されている ATM (automatic teller machine) 等を用いて自己の銀行預金残高の全部または一部に対応する金額データを IC カードのメモリ領域に格納しておき、商品購入時には、店舗にあるオフライン端末を用いて上記金額データを逐次減算していく場合がオフライン取引に該当する。

【0003】 このようなオフライン取引においては、IC カードに格納されている金額データと、センタシステム側で管理している預金残高に相当する金額データとの不一致による、カード発行者とカード保有者との間のトラブル発生を回避する手段を講じることが重要となる。

【0004】 そこで、従来は、カード内部の金額データを先に更新し、次いでオンラインによって銀行口座の預金残高を更新するという手順がとられている。あるいは、逆に、銀行口座の預金残高を更新してから、カード内部のデータを後で更新するという手順がとられる場合もある。カード内部の金額データを更新する場合は、1 回のデータ更新要求コマンドにより、カード内部のデータを更新するとともに必要に応じてその履歴をカード内

部に追記していた。

【0005】 図 10 は、IC カード側とセンタシステム側との金額データの不一致を防止するための手順を示したシーケンスチャートであり、IC カード、ATM に設けられるカードリーダライタ（以下、R/W）、及び、ATM にオンライン接続されているセンタシステムにおける、それぞれの処理の流れを示すものである。

【0006】 図 10 において、R/W (ATM) は、挿入されている IC カードに対して現在の金額データの更新要求（更新データ+コマンド）を行う（R41、R42）。IC カードは、この更新要求の受信によって自己のメモリ領域に格納されている金額データを更新し（K41）、併せて更新履歴をメモリ領域に追記する（K42）。正常終了した場合は、更新済通知を R/W 側へ送る（K43）。IC カードから更新済通知を受信した R/W は（R43）、センタシステムに対して管理データの更新要求（更新データ+コマンド）を行う（R43）。ここに管理データとは、当該 IC カードの正規所有者について管理している金額データをいう。センタシステムは、管理データ更新要求の受信により該当する管理データを検索して更新し（C41）、それが正常終了した場合は、更新済通知を R/W に送る（C42）。この通知を受信した R/W は、図示しないディスプレイ等に更新済を表示した後（R44）、当該 IC カードの排出制御を行う（R45）。このようにして、IC カードの金額データとセンタシステム側で管理している金額データとの連携が図られている。

## 【0007】

【発明が解決しようとする課題】 ここで、金額データを増やす場合を想定する。また、この場合のデータ更新手法として、IC カード側の金額データを更新（増額）した後に、センタシステム側の管理データを更新（増額）する手法を採用していたとする。このような状況では、IC カードにおけるデータ更新は正常に終了し、それにより金額データは増えたが、オンラインによるセンタシステム側のデータ更新が正常に行われなかった場合は、それを知らないカード所有者が、センタシステム側の管理データを越える金額で IC カードによる買い物をしてしまうことが考えられる。

【0008】 また、その逆に、IC カード内部の金額データを減らす場合、センタシステム側の管理データを更新（減額）した後に IC カード側の金額データを更新（減額）する手法を採用していたとする。このとき、センタシステム側のデータ更新は正常に終了し、それにより管理データは減ったが、IC カード内部のデータ更新が何らかの理由で正常に実行できなかった場合には、正常に減額がなされたと信じているカード所有者が、センタシステム側の管理データを越える金額で IC カードによる買い物をしてしまうことが考えられる。

【0009】 つまり、従来の IC カードでは、オフライ

ン取引の際に、カード内部の金額データとセンタシステム側の管理データとの不一致を生じる可能性が高く、正しい金額データの使用が保証されにくいという問題があった。

【0010】そこで、本発明の課題は、カード内部の格納データの更新状態とその格納データを管理している側の更新状態との不一致の発生、及び該不一致状態でのカード取引を自律的に抑制することができるICカード、及びこのICカードを用いたICカードシステムを提供することにある。

【0011】

【課題を解決するための手段】上記課題を解決するため、本発明は、IC内部のデータ格納領域に格納されたデータの更新制御手段を有するICカードと、このICカードの格納データに対応する内部管理データの更新制御手段を有する第1装置と、前記ICカード及び第1の装置の各更新制御手段に対してデータ更新要求を発行する第2装置とを含んで構成されるICカードシステムにおいて、前記第2装置に、前記ICカードの更新制御手段へ前記格納データの仮更新を要求する仮更新要求発行手段と、該仮更新の正常終了を確認したときに前記第1装置の更新制御手段へ内部管理データの実更新を要求する実更新要求発行手段と、該内部管理データの実更新の正常終了を確認したときに前記ICカードの更新制御手段へ本更新を要求する本更新発行手段とを設け、この本更新の実行によって前記ICカード内の格納データの内容を確定させるようにした。

【0012】このICカードシステムのより好ましい形態としては、前記第2装置に、さらに、前記内部管理データの実更新の異常の有無を監視するシステム監視手段と、該システム監視手段が異常を検知したときに前記本更新の要求に代えてリカバリ要求を前記ICカードの更新制御手段へ送出するリカバリ要求発行手段とを設ける。この場合、前記ICカードの更新制御手段は、前記リカバリ要求の受信時に前記仮更新の実行前の状態を復元するように構成する。

【0013】本発明は、また、上記ICカードシステムでの利用に適したICカードを提供する。このICカードは、下記の機能をもつ更新制御手段を有することを特徴とするものである。

(1) IC内部のデータ格納領域内の格納データについての仮更新要求を受信したときに該仮更新要求に基づく更新候補データを生成する第1の手段と、生成された前記更新候補データについての本更新要求を受信したときに該更新候補データの内容を確定させる第2の手段。

(2) 前記仮更新要求の受信を契機に少なくとも前記データ格納領域へのアクセスを制限させ、前記本更新要求の受信を契機に該制限を解除する第3の手段。

(3) 所定のリカバリ要求の受信を契機に前記データ格納領域内の格納データを前記仮更新要求前の状態に復元

させるリカバリ要求実行手段。

(4) 前記仮更新要求の実行結果または前記更新候補データの元データを一時的に保持するデータバッファと、前記本更新要求またはリカバリ要求の受信時に前記データバッファの保持内容をクリアするバッファ制御手段。つまり、IC内部の格納データとこれを管理する側のデータとの不一致の有無を検知し、一致性の確認が確保できない間の更新候補データの使用を制限するとともに、本更新要求時またはリカバリ要求時の後続処理の迅速化を図ることができるICカードを提供する。

【0014】

【発明の実施の形態】以下、図面を参照して、本発明の実施の形態を詳細に説明する。図1は、本発明が適用されるICカードの構成例を示す図である。このICカード1は、カードリーダーライタ(R/W)2との間のデータ入出力制御を行う入出力制御部(I/O)11、マイクロプロセッサ(CPU)12、ROM13、RAM14、及びEEPROM15を備えて構成される。

【0015】RAM14は、CPU12がプログラムを実行するために使用するワーキングメモリであり、ROM13は、少なくともCPU12が実行する制御プログラムを格納するメモリである。この実施形態では、CPU12、ROM13、及びRAM14によって本発明の更新制御手段を実現する。

【0016】図2は、EEPROM15の内容説明図である。本実施形態では、EEPROM15に、少なくとも、PIN(Personal Identification Number: 暗証番号)の現在の設定状態がPINロック状態かPINアンロック状態かを表すカードステータスを格納するためのステータス格納領域151、変更データバッファ152、金額データ格納領域153、及び更新履歴格納領域154を形成している。なお、このほか、必要に応じてPINの格納領域を別途形成しておいてもよい(複数のPINを設定する場合等)。

【0017】PINロック状態とは、金額データへのアクセス時(データ保存、更新、読出し等、以下同じ)、保有者PINの入力を促して利用者認証を行うことを必須とする状態であり、カードステータスがこの状態のときは、カード使用時にPIN入力が必要となる。一方、PINロック解除状態とは、操作上の便宜を考慮してPIN入力を不要としている状態、つまり、PINによる利用者認証が省略される状態である。カードステータスがこの状態のときはカード使用時のPIN入力は不要となる。

【0018】変更データバッファ152は、例えば金額データ格納領域153に格納されるデータを外部(R/W2)から受信したデータをもとに生成(算出)する場合、この受信データ等を一時的に保持しておき、その内容が確定したとき、あるいは最終的に確定し得なかったときに、保持データをもとに金額データ格納領域153

内の金額データを元に戻す、という場合に使用される。

【0019】更新履歴格納領域154は、金額データの更新が確定する度にその取引日と額の履歴を追記するための領域である。この更新履歴は、後日の取引行為の分析時等に使用されるものである。

【0020】図3は、ROM13に格納された制御プログラムに従ってCPU12により実現される更新制御手段の機能ブロック構成図である。この実施形態では、更新要求実行処理部121、演算処理部122、データ・履歴状態判定部123、ステータス遷移制御部124、バッファ制御部125、データ更新処理部126、及び更新履歴追記処理部127を構築する。更新要求実行処理部121は、下記の各部122～127の制御を統括するものであり、I/O11を介してR/W2から入力される各種要求（コマンド）や金額データ等を識別し、現在のカードステータスを監視しながら入力された各種要求の実行等を行う。例えば、カードステータスがPINロック状態のときはPIN入力による照合以外は特定のコマンド入力がないと金額データへのアクセスを禁止するようにする。このデータアクセスの禁止状態を単なる「ロック状態」と称し、PINロック状態とは区別して説明する。但し、後述の本更新要求やリカバリ要求については、ロック状態であってもこれを受け付けて実行するように例外コマンドを設定しておく。

【0021】演算処理部122は、金額データの演算の際に用いられるものである。データ・履歴状態判定部123は、現在の金額データや履歴の状態が仮状態（更新可能であるが未確定の状態、以下同じ）か本状態（更新が確定している状態、以下同じ）かを判定する。この判定は、例えば、変更データバッファ152内にデータが保持されていれば仮状態、保持データが存在しておらず、金額データ格納領域153の金額データや変更履歴格納領域154内の更新履歴の内容が確定している場合は本状態と判定する。変更バッファメモリ152内の保持データ、あるいは金額データ格納領域153の金額データや変更履歴格納領域154内の更新履歴に仮状態または本状態のフラグを立てておくことで判定するようにしてもよい。

【0022】ステータス遷移制御部124は、更新要求実行処理部121の指示によってステータス格納領域151の現在のカードステータスの監視と遷移制御を行う。この実施形態では、金額データ等が仮状態のときは当該金額データに対するアクセスを制限するためにロック状態にしておき、本状態になったときにロック解除状態に遷移させるものとする。

【0023】バッファ制御部125は、変更データバッファ152のクリア等を行うものである。データ更新処理部126は、金額データ格納領域153に格納されている金額データの更新等を行うものであり、更新履歴追記処理部127は、更新履歴格納領域154内の更新履

歴を追記するものである。なお、更新履歴格納領域154内の更新履歴は上書きするように変更してもよい。

【0024】次に、上記ICカード1との間でデータ等の授受を行うR/W2（第2装置）側の構成を説明する。この場合のR/W2は、例えば図示しないセンタシステム側とオンラインで結ばれたATMやPOS操作端末等に備えられるものを想定している。

【0025】R/W2は、更新管理部21と、コマンド発行部22と、システム監視部23とを含んで構成される。更新管理部21は図示しないテンポラリメモリを有し、R/W2の操作者、ICカード1、及びセンタシステムから、金額データ、更新データ、各種通知、あるいは後述のシステム監視結果等を受け取ってテンポラリメモリに一時的に格納するとともに、各種通知やデータ更新に関する情報を出力ないし返送する。また、テンポラリメモリの格納データに基づいてコマンド発行部22に各種要求発行の指示を与える。コマンド発行部22は、ICカード1に対して仮更新要求及び本更新要求（データ込）、あるいはリカバリ要求を生成して送信するとともに、センタシステム側に管理データの実更新要求を生成して送信するものである。

【0026】仮更新要求は、ICカードに金額データの仮更新を要求するためのコマンドであり、例えばカード取引時に入力される金額データの関連データ（例えばセンタシステムに送信した更新データ）が更新管理部21のテンポラリメモリに存在しない場合に、これを検知した更新管理部21からの指示によって生成される（仮更新要求発行手段）。

【0027】また、本更新要求は、ICカードに仮状態にある金額データの確定を要求するコマンドであり、センタシステムからの更新済通知の受信時にテンポラリに該当更新データが存在する場合に、これを検知した更新管理部21からの指示によって生成される（本更新要求発行手段）。

【0028】一方、リカバリ要求は仮更新要求を発行した後に何らかの理由でセンタシステム側での管理データの実更新が成功しなかった場合にICカード1の内容を仮更新要求の発行直前の状態に復元させるためのコマンドであり、仮更新処理の正常終了後に本更新要求を発行できない事態の発生を検知した更新管理部21からの指示によって生成される（リカバリ要求発行手段）。

【0029】システム監視部23は、例えばタイマを含んで構成され、コマンド発行部22がセンタシステムへ管理データ更新要求を発出した後の経過時間を監視し、タイムアップ前に更新済通知を受領しない場合にその結果を更新管理部21に通知するように構成される（システム監視手段）。

【0030】次に、R/W2から上記各種要求（コマンド）を受信したときのICカード1側の処理動作を図5及び図6を参照して説明する。図5は、仮更新要求を受

信した場合の例である。この場合は、まずカードステータスを調べ、ロック解除状態になっている場合は、ロック状態へ遷移させる(ステップS101、102、103)。次いで、変更データバッファ152がクリア状態かどうかを確認し、クリア状態であれば、対象金額データが本状態かを調べ、本状態であれば最新更新履歴が本状態であるかどうかを調べる(ステップS104、105、106)。最新更新履歴が本状態のときは変更データバッファへ仮更新要求と共に送られたデータを書き込み(ステップS107)、更新候補データの算出を行う(ステップS108)。そして、金額データ格納領域153内の金額データの仮更新と更新履歴格納領域154内の更新履歴の仮追記とを行い(ステップS109、110)、正常処理済通知をR/W2側に送る(ステップS111)。ステップS103、104、105、106での判定結果が否定的である場合はエラー処理、例えば正常に仮更新できなかった旨のレスポンスをR/W2側に送る。

【0031】図6は、本更新要求を受信した場合の例である。この場合は、カードステータスを調べ、ロック状態であることを確認する(ステップS201、202)。ロック状態であれば変更データバッファ152に有効なデータ、すなわち本更新の際に用いられるデータが存在しているかどうかを調べる(ステップS203)。有効なデータの存在を確認した場合は、対象金額データが仮状態かどうかを調べ、仮状態であれば最新更新履歴が仮状態かどうかを調べる(ステップS204、205)。仮状態であれば該当する金額データの本更新と更新履歴の本追記とを行う(ステップS206、207)。その後、変更データバッファ152の内容をクリアし(ステップS208)、ロック状態を解除させるとともに(ステップS209)、正常処理済通知をR/W2側に対して行う(ステップS210)。一方、ステップS202、203、204、205での判定結果が否定的である場合は、上述のエラー処理をR/W2に対して行う(ステップS211)。

【0032】なお、以上は、仮更新要求の中にICカードをロックする機能、本更新要求の中にICカードのロックを解除する機能が含まれていることを前提として説明したが、これらの機能は、各更新要求とは別のコマンドにより行うことができる。

【0033】次に、上記のように動作するICカード1、R/W2、及びセンタシステム側の処理の全体の流れを図7～図9を参照して説明する。

【0034】図7は、正常時の流れを示すシーケンスチャートである。R/W2が仮更新要求を送信した後(R11、R12)、ICカード1から正常処理済通知を受信するまでの手順(K11～K14)については図5に示したとおりである。ICカード1側の仮更新処理が正常に終了した場合、R/W2は、次に、センタシステム

に対して管理データの実更新要求(更新データ込)を送信する(R13)。センタシステムでは、該当する管理データを検索してこれを更新し(C11)、更新済通知をR/W2に送る(C12)。この通知により管理データの実更新を確認したR/W2は(R14)、ICカード1に対して本更新要求を送信する(R15)。この本更新要求を受信したICカード1が対象金額データや更新履歴の本更新、本追記を行った後、ロック状態の解除をR/W2に通知するまでの手順(K15～K19)は、図6に示したとおりである。解除通知を受けたR/W2は、正常処理済をディスプレイ等に表示し(R16)、所要の終了処理を経てカード排出制御を行う(R17)。

【0035】図8は、異常時の流れを示すシーケンスチャートである。異常発生形態としては種々のものが考えられるが、ここでは、センタシステム側において実更新ができない原因が発生し、前述の更新済通知(C12)がR/W2側に送信されなかったものとする。

【0036】この場合、R/W2が仮更新要求をICカード1側に送信するとともに、ICカード1から正常処理済通知を受信したR/W2がセンタシステムに管理データの実更新要求を送信するまでの手順(R21、R22、K21～K25、R23)は図7の場合と同様である。ここでは、R/W2において、管理データの更新要求送信と同時にタイマによる監視を始める(R24)。この監視は、システム監視部23が行う。上述のようにセンタシステムに異常が発生しているので(C21)、タイムアップ後も更新済通知は行われず(R25)。そこで、システム監視部23は、監視結果が否定的であることを更新管理部21に伝える。更新管理部21は、この監視結果に基づいてエラー処理、例えば図示しないディスプレイにエラー表示を行う(R27)。このように、仮更新要求後、本更新要求前に異常が発生した場合、ICカード1の金額データや更新履歴は仮状態のままであり、カードステータスもロック状態が継続される。

【0037】図9は、リカバリ処理時のシーケンスチャートである。リカバリ処理は、ICカード1の金額データ等が仮状態を維持しているときに、これを仮更新要求の直前の状態に強制的に復元するものである。このリカバリ処理は、R/W2からICカード1へリカバリ要求が送信されることによって開始する(R31、R32)。ICカード1では、更新要求実行処理部121が、金額データ格納領域153内の金額データに変更データバッファ152上の変更金額データを加算(仮更新が減額であった場合)、または減算(仮更新が増額であった場合)する(K31)。また、最新のデータ更新仮履歴を削除する(K32)。その後、変更データバッファ152をクリアし(K33)、ロック状態を解除するとともに、ロック状態解除をR/W2に通知する(K3

4)。R/W2は、このロック状態解除をディスプレイ等に表示した後(R33)、カード排出制御を行う(R34)。これにより、ICカード1は、仮更新要求前の状態に戻る。

【0038】このように、本実施形態のICカード1は、センタシステムにおける管理データとの不一致を検知するとともに、そのような状態での使用が防止される機能を有しているので、カード所有者が、センタシステム側の管理データを越える金額で買い物をしてしまう事態を回避することができる。

【0039】なお、本実施形態では、金額データの場合の例を挙げて示したが、このほか、図書カードによる貸出量や、ゲームカードによる得点量の場合も同様の実施態様が可能である。

【0040】

【発明の効果】以上の説明から明らかなように、本発明のICカードによれば、センタシステム側の管理データとの連携が図られるので、該管理データと不一致の状態でのICカードによる取引が回避される効果がある。このような効果は、オフライン取引を許容するICカードシステムでは、特に有効となるものである。

【図面の簡単な説明】

【図1】本発明が適用されるICカードの構成図。

【図2】本実施形態のICカードのEEPROMの内容説明図。

【図3】本実施形態のICカードにより実現される機能ブロックの構成図。

【図4】本実施形態のカードリーダライタ側が備える機能ブロックの構成図。

【図5】本実施形態において仮更新要求を受信した場合のICカード側の処理順の説明図。

【図6】本実施形態において本更新要求を受信した場合

のICカード側の処理手順の説明図

【図7】本実施形態のICカード、R/W、及びセンタシステムにおいて、正常時の処理の流れを示すシーケンスチャート。

【図8】本実施形態のICカード、R/W、及びセンタシステムにおいて、異常発生時の処理の流れを示すシーケンスチャート。

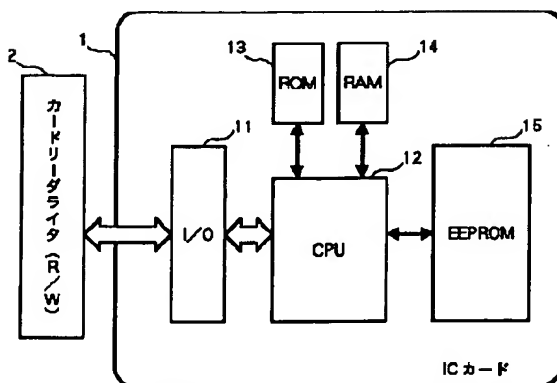
【図9】本実施形態のICカード、R/W、及びセンタシステムにおけるリカバリ処理の流れを示すシーケンスチャート。

【図10】ICカード、R/W、及びセンタシステムにおいてデータ更新要求が発生した場合の従来の処理の流れを示すシーケンスチャート。

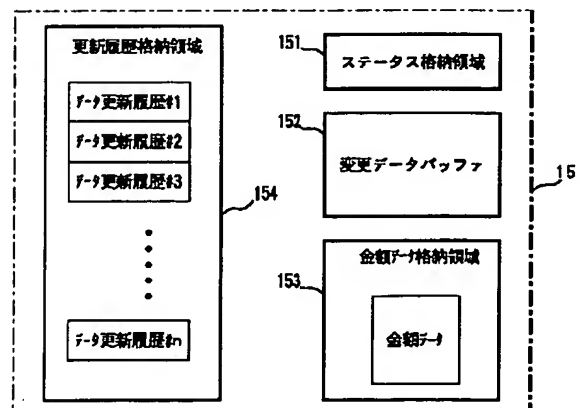
【符号の説明】

- 1 ICカード
- 2 カードリーダライタ(R/W)
- 11 入出力制御部(I/O)
- 12 マイクロプロセッサ(CPU)
- 13 ROM
- 14 RAM
- 15 EEPROM
- 121 更新要求実行処理部
- 122 演算処理部
- 123 データ・履歴状態判定部
- 124 ステータス遷移制御部
- 125 バッファ制御部
- 126 データ更新処理部
- 127 更新履歴追記処理部
- 151 ステータス格納領域
- 152 変更データバッファ
- 153 金額データ格納領域
- 154 更新履歴格納領域

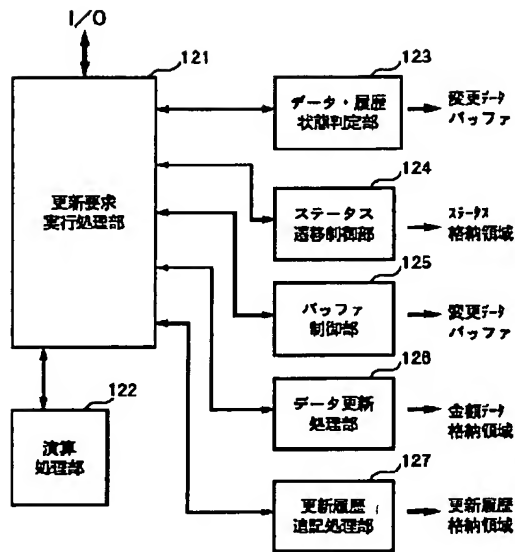
【図1】



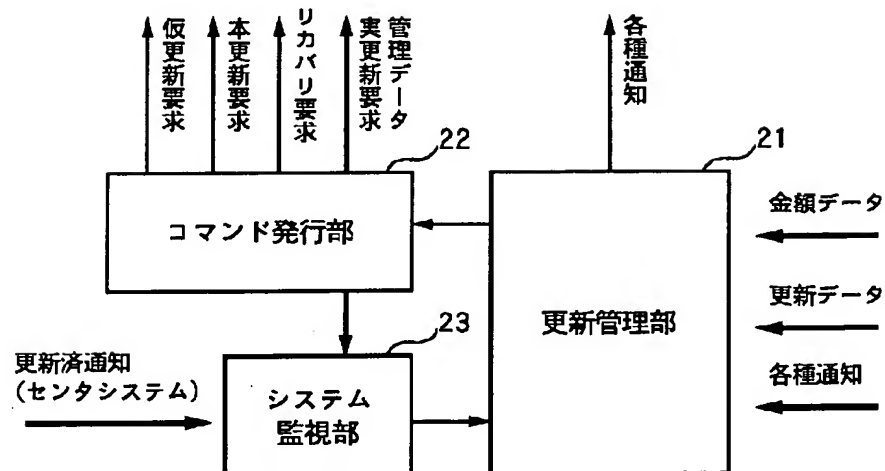
【図2】



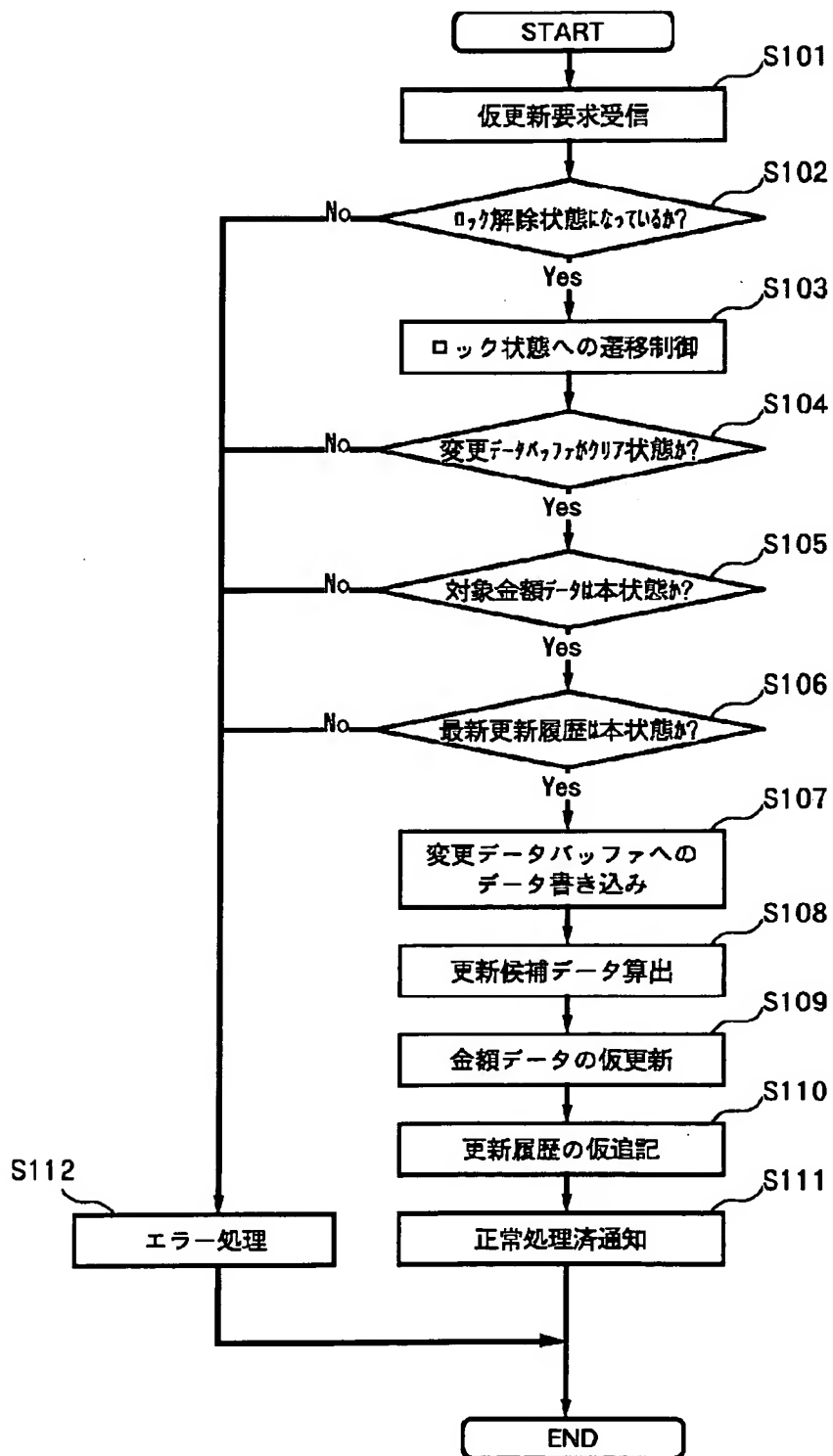
【図 3】



【図 4】

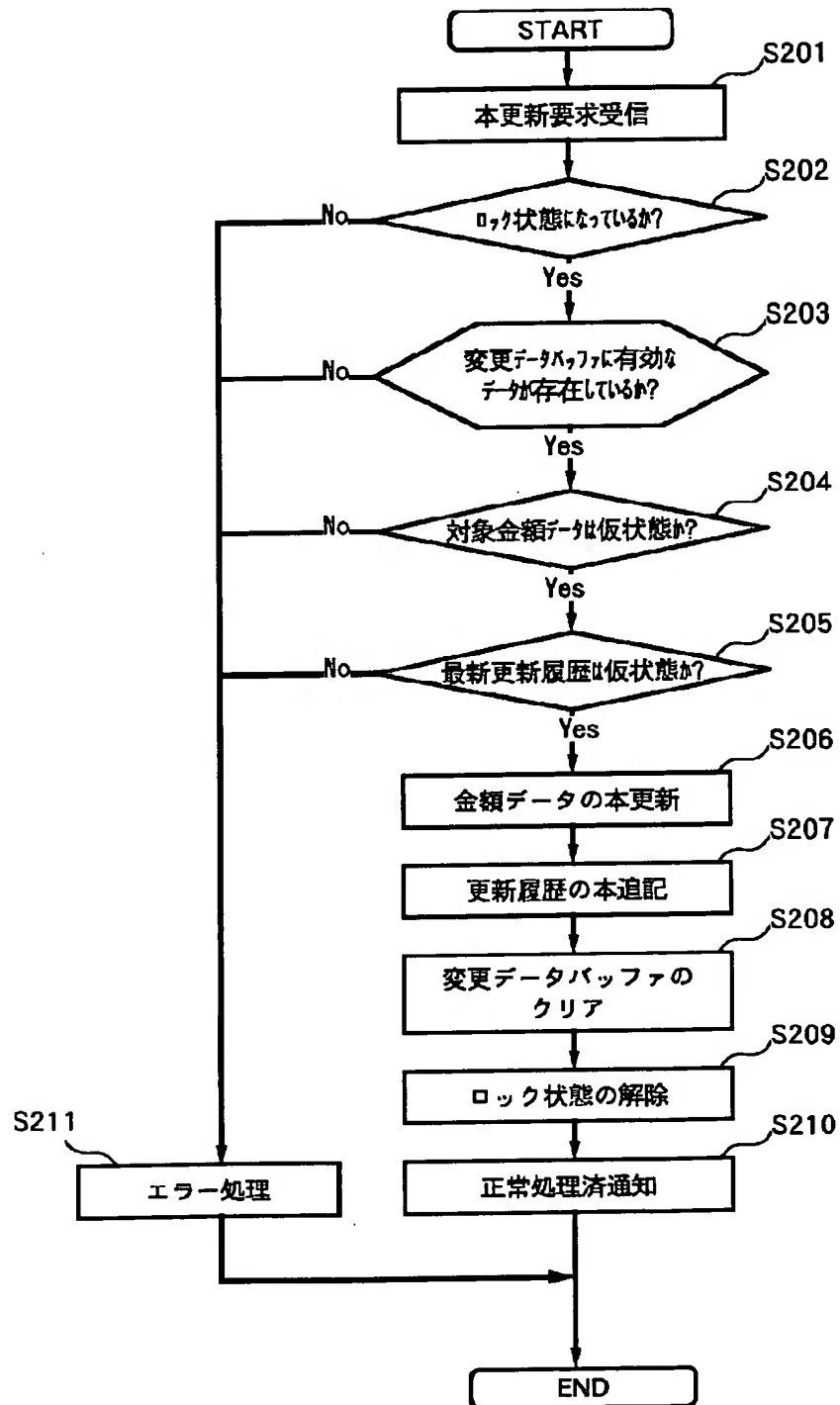


【図 5】

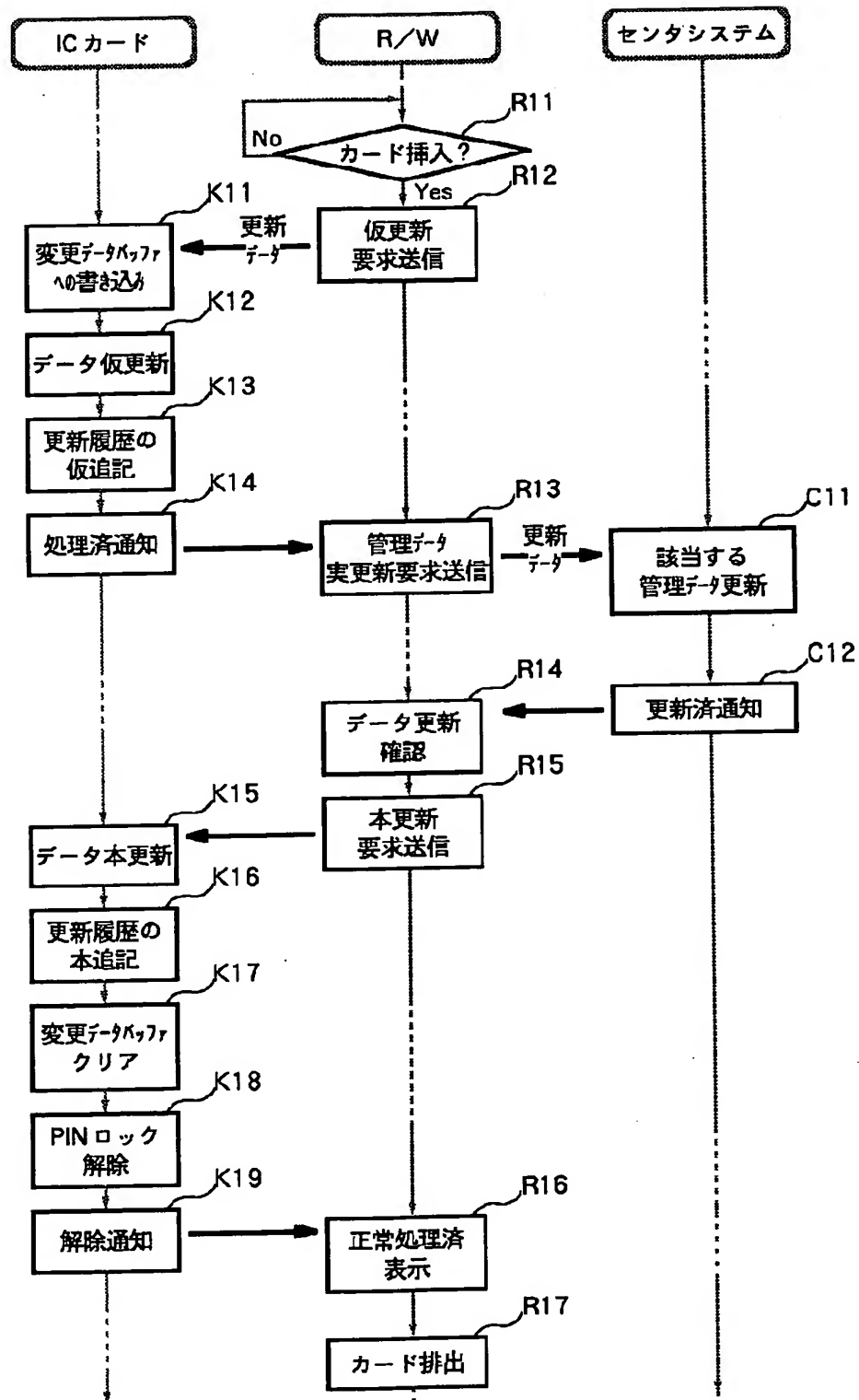




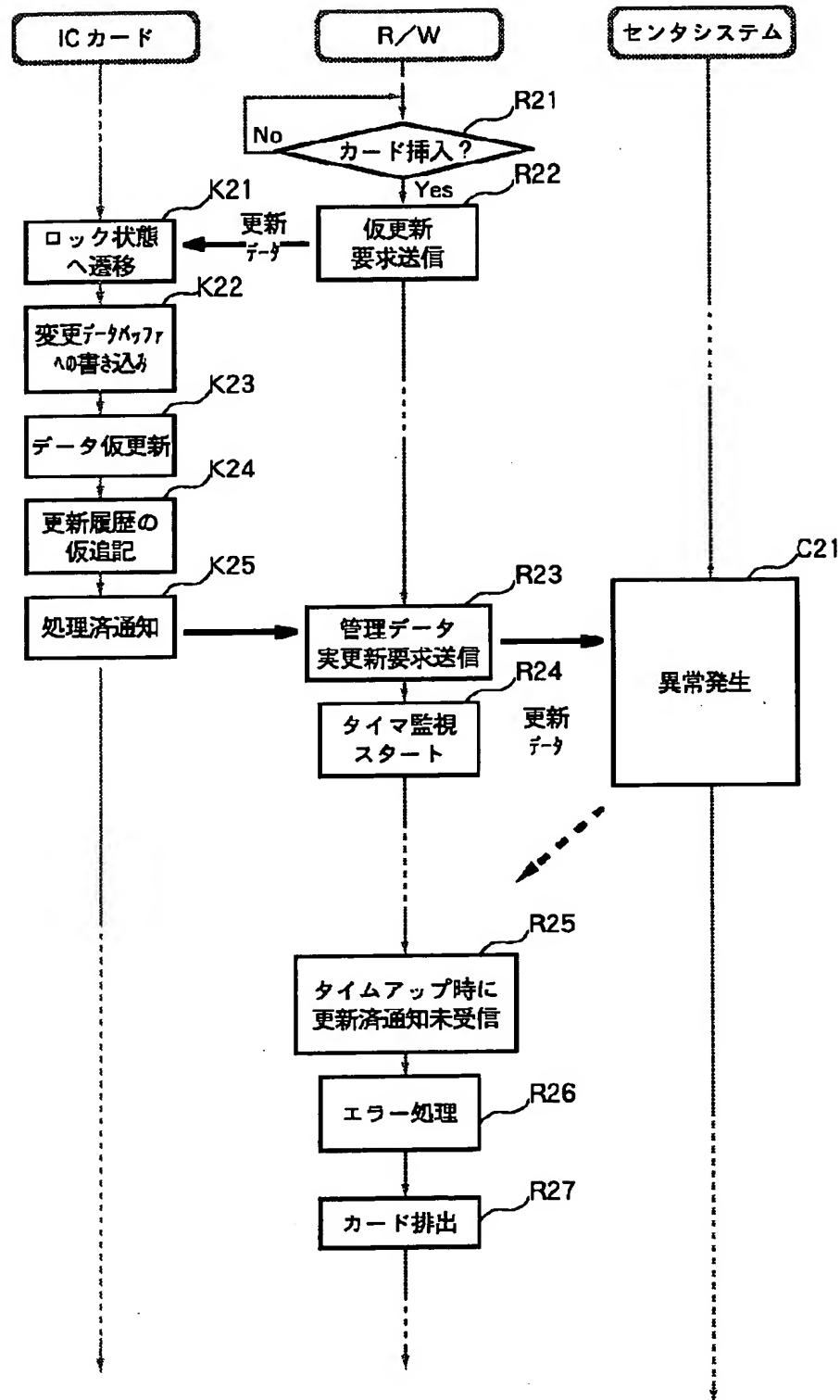
【図 6】



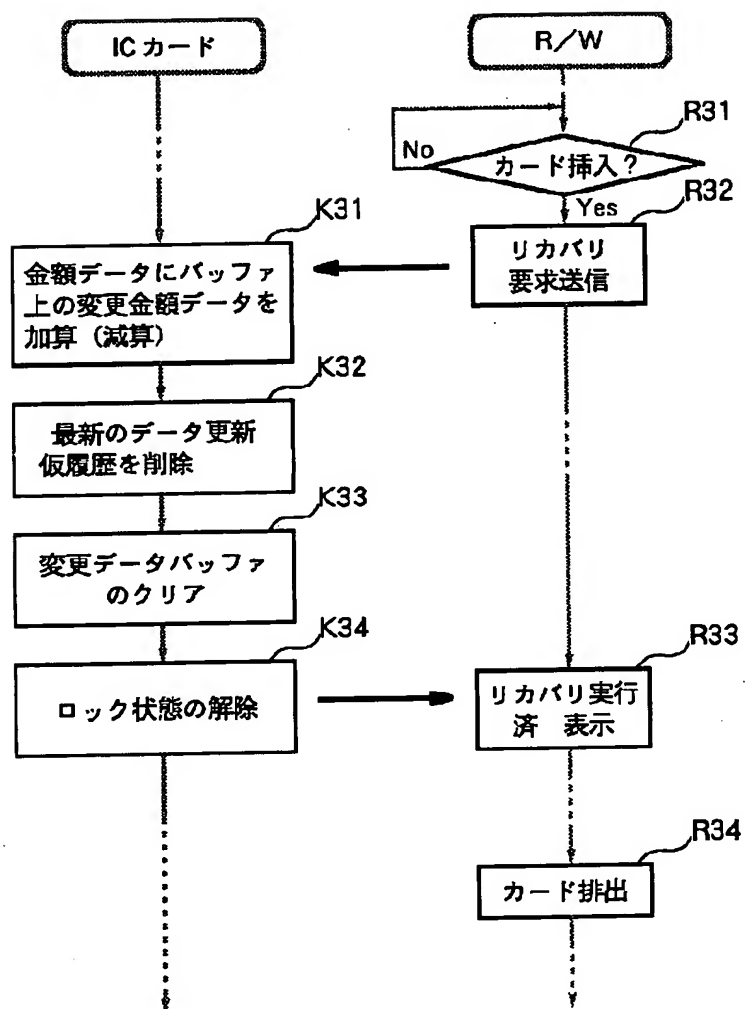
【図 7】



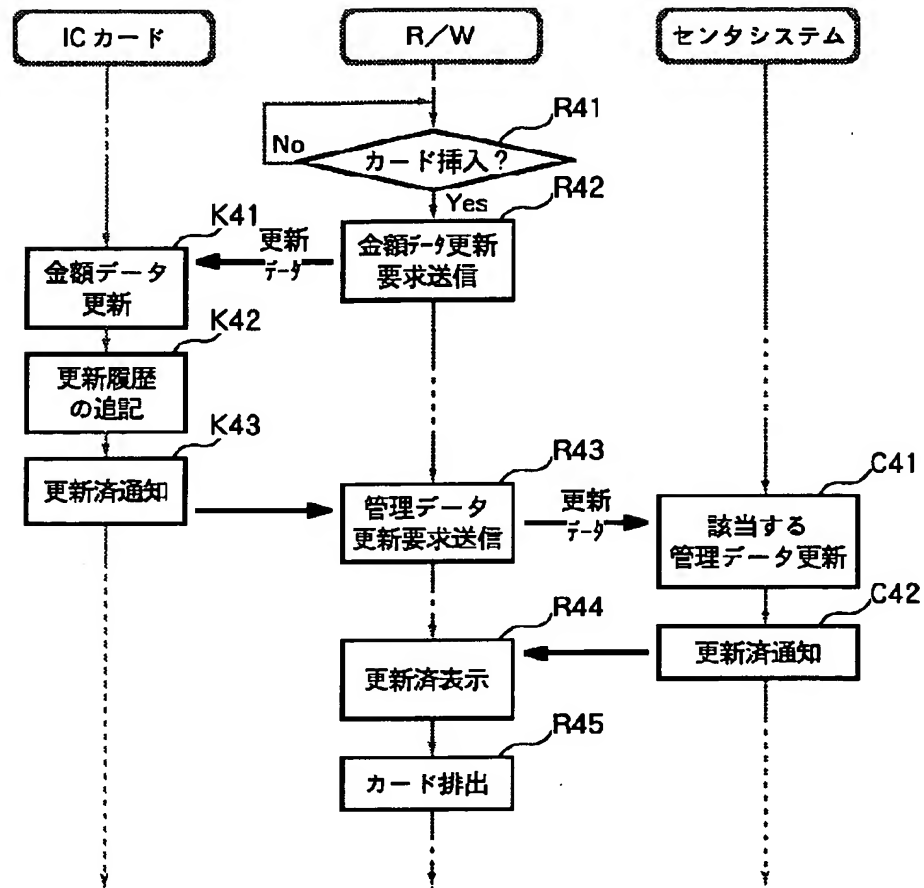
【図 8】



【図 9】



【図 10】



フロントページの続き

(51) Int. Cl. <sup>7</sup>  
19/10

識別記号

F I

データコード (参考)

P

(72) 発明者 重木 昭信  
東京都江東区豊洲三丁目3番3号 株式会  
社エヌ・ティ・ティ・データ内

(72) 発明者 今井 考司  
東京都江東区豊洲三丁目3番3号 株式会  
社エヌ・ティ・ティ・データ内

Fターム(参考) 5B035 AA13 BB09 BC00 CA29  
5B058 CA26 KA08 KA31 KA33  
5B082 GA14 GB02 GB04

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**